REMARKS

Claims 8, 15, 17 and 20 have been amended for consistency. No new matter has been added. Claims 1-12 and 14-26 are pending in the application. Applicant reserves the right to pursue the original claims and other claims in this and other applications.

Claims 1, 6-8, 14-20 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki et al. (U.S. Pat. Pub. No. 2003/0078072) ("Serceki") in view of Linkola et al. (U.S. Pat. No. 6,934,931) ("Linkola"). This rejection is respectfully traversed.

Claim 1 recites:

> A method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising:
>
> physically separating from said wireless station a network communications device;
>
> physically connecting said separated network communications device to an encryption key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device;
>
> replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network;
>
> physically reconnecting said network communications device containing said new encryption key with said wireless station of said network; and
>
> accessing said new encryption key on said network communications device during an encrypted communication.

Serceki is essentially a method of transferring information between two computers systems that are not physically connected by using a storage device as a conduit between the two systems, e.g., a "wireless station" and a "wired portion of a network." Thus, in the invention of

Serceki, a storage device is used to transfer data, e.g., configuration information or security keys, between the two computer systems. The Office Action admits that Serceki fails to disclose at least "accessing said new encryption key on said network communication device during an encrypted communication." (Office Action at pgs. 2-3). Linkola, which relates to cellular telephone technology, discloses a system for wirelessly changing the identity module station identity (IMSI) on a subscriber identity module (SIM). (Linkola, Abstract). An IMSI is a unique identifier which is used to link a phone number to a mobile handset—different from an encryption key that may be used during encrypted communications. Accordingly, Linkola does not cure the deficiencies of Serceki.

Linkola is cited by the Office Action as allegedly disclosing "accessing said encryption key on said network device during an encrypted communication." (Office Action at pgs. 2-3, 6). Applicant respectfully disagrees, and even assuming that this statement were true, the Office Action fails to address the fact that claim 1 recites "accessing said new encryption key on said network device during an encrypted communication." The distinction that the encryption key must be new is critical. Though Linkola discloses that an encrypted code key K_1 is stored on a mobile station's SIM "for encryption of wireless… communication," when the control device of Linkola performs a phone number/IMSI change or addition, the encrypted code key K_1 does not change. (Linkola, col. 5, lns. 1-39; col. 6, lns. 34-67). Only a new phone number/IMSI is transmitted to the mobile station. (Linkola, col. 5, lns. 22-40). Thus, even if K_1 is accessed during a subsequent encrypted communication, which applicant does not concede, K_1 is not new. Accordingly, neither Linkola nor Serceki disclose, teach or suggest "accessing said new encryption key on said network device during an encrypted communication."

Furthermore, Linkola teaches away from Serceki and the references therefore are not combinable. Conventional understanding dictates that wirelessly changing the encryption key on a SIM for a wireless communication device is undesirable because of the risk that the encryption key could be intercepted and the data cloned, leading to potentially fraudulent use of the wireless telecommunications network. *See, e.g.*, U.S. Patent No. 5,309,501 to Kozik, et. al, at col. 2, lns. 1-20; col. 22, lns. 5-27 (discussing that an encryption key is never transmitted over the air). This is

one of the primary reasons that SIM cards, which contain embedded integrated circuits for encrypting data using the stored encryption key, are used in wireless telephones instead of internal memory.

Moreover, Linkola specifically teaches updating information (which does not include an encryption key) on the mobile handset wirelessly, whereas claim 1 specifically requires that the wireless communications device be disconnected from the wireless network to receive a new encryption key. Even assuming the references could be combined, which applicant does not admit, Linkola teaches away from updating information on mobile handsets disconnected from the wireless network. Specifically, updating Linkola's mobile handset requires using wireless SMS short messages for communication between the handset and control device. (Linkola, col. 5, lns. 23-40). Accordingly, one of ordinary skill in the art would not modify Serceki with the teachings of Linkola. As such, for both these reasons and the reasons discussed above, the rejection of claim 1 should be withdrawn and the claim allowed.

Claims 6-7 depend from claim 1 and are allowable for at least the reasons noted above with respect to claim 1.

Claims 8, 15, 17, 20 recite similar limitations as claim 1, *e.g.*, "said wireless network communications device being physically disconnectable from said wireless station and physically connectable to said wired encryption key updating device wired to said network to receive, store, and use a new encryption key," (Claim 8, emphasis added), "said removable wireless network communications device being physically connectable to a wired network to receive, store, and use a new encryption key," (Claim 15, emphasis added), "said wireless station configured to access said new encryption key on said wireless network communications device during a wireless communication," (Claim 17, emphasis added), and "said new encryption key on said wireless network communications device being accessible by a wireless network device during encrypted communications," (Claim 20, emphasis added), and are allowable for at least the reasons noted above with respect to claim 1. Claims 14, 16, 18-19 and 26 depend from claims 8, 15, 17, and 20

respectively, and are likewise allowable. Accordingly the rejection of those claims should be withdrawn and the claims allowed over the Serceki and Linkola combination.

Claims 2-3, 9-10, and 21-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki in view of Linkola and in further view of U.S. Pat. No. 4,369,332 to Campbell, Jr. ("Campbell"). This rejection is respectfully traversed.

Claims 2-3, 9-10, and 21-23 recite similar limitations to claim 1 and are allowable over the combination of Serceki and Linkola for at least the reasons noted above with respect to claim 1.

Campbell discloses:

> "[An] apparatus and method for generating a unique working key variable for controlling the operation of an encryption/decryption device during each user specified time period. The apparatus generates each working key variable by encrypting a user specified value, unique for each specified time period, under control of a fixed key variable stored in the apparatus. After the user specified value has been encrypted, the apparatus utilizes the encrypted (working) key variable to control the encryption/decryption of data during the corresponding user specified time period." (Campbell, Abstract)

Campbell fails to disclose "accessing said new encryption key on said network device during an encrypted communication." (emphasis added). As such, Campbell fails to cure the deficiencies of Serceki and Linkola. Therefore the rejection of claims 2-3, 9-10, and 21-23 should be withdrawn and the claims allowed.

Claims 4-5, 11-12 and 24-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki in view of Linkola and in further view of U.S. Pat. No. 6,226,750 to Trieger ("Trieger"). This rejection is respectfully traversed.

Claims 4-5, 11-12 and 24-25 recite similar limitations to claim 1 and are allowable over the combination of Serceki and Linkola for at least the reasons noted above with respect to claim 1.

Trieger discloses:

> "[A] method and system for tracking communications in a client-server environment. The method includes the steps of sending a first request from the client to the server over a first connection, sending a first key from the server to the client over the first connection, sending the first key from the client and a second request to the server over a second connection, and sending a response to the second request and a second key distinct from the first key from the server to the client over the second connection. The system includes a client for establishing a terminal connection with a server and a server in communication with the client. The server further includes key generator means generating a plurality of keys for transmission to the client, authentication means in communication with the key generator means receiving the keys from the client to recognize the keys at the server, and discarding means linked to the key generator means for disposing of previously transmitted keys." (Trieger, Abstract)

Like Serceki and Linkola, Trieger also fails to disclose at least "accessing said new encryption key on said network device during an encrypted communication." (emphasis added). As such, Trieger fails to cure the deficiencies of Serceki and Linkola. Therefore, the rejection of claims 4-5, 11-12 and 24-25 should be withdrawn and the claims allowed.

In view of the above, applicant believes the pending application is in condition for allowance.

Dated: March 5, 2008

Respectfully submitted,

By MAW #41,194

Thomas J. D'Amico
Registration No.: 28,371
Michael A. Weinstein
Registration No.: 53,754
DICKSTEIN SHAPIRO LLP
1825 Eye Street, NW
Washington, DC 20006-5403
(202) 420-2200
Attorneys for Applicant